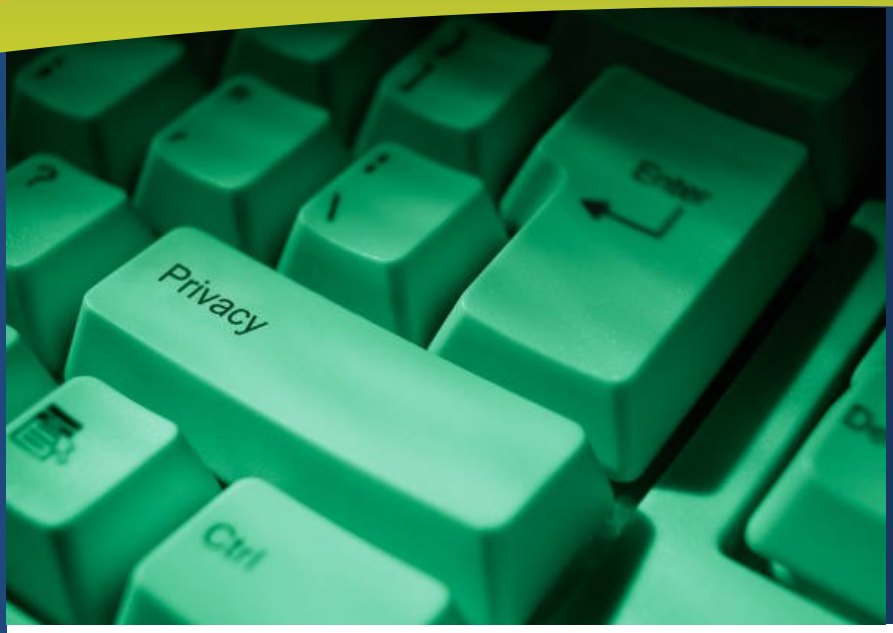
Information Technology Laboratory Newsletter



May—June 2015

Issue 135

INSIDE THIS ISSUE

NSTIC Announces Privacy Pilot Funding

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative signed by President Obama in 2011 to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions. One of the NSTIC key initiatives is pilot projects—designed to catalyze the marketplace of solutions and infrastructure. The pilot projects have enabled significant technological, business, and policy advances across the public and private sectors by identifying and addressing challenges in the Identity Ecosystem. In addition to accelerating the emergence of a commercial market, the pilots have helped to advance the infrastructure of the Identity Ecosystem.

As the pilot program evolves, the pilots' work will continue to be available as a resource to other organizations in the field, highlighting common themes, challenges, and successes. The NSTIC pilots will continue to inform the broader Ecosystem of their experiences and will assist the private sector in creating the Identity Ecosystem Framework. They will also continue to catalyze development of the Identity Ecosystem by creating viable solutions and growing the marketplace for identity federation.

The NSTIC National Program Office (NPO) recently announced a new pilot program initiative with a special focus on turning privacy-enhancing technologies (PETs) into commercially viable solutions—the first NPO effort to dedicate funding toward a single aspect of identity solutions. The privacy-enhancing NSTIC guiding principle addresses concerns that the development of more trusted and federated identity solutions could create risks for privacy and civil liberties—such as increased tracking and profiling of individuals. But barriers exist to the implementation of PETs that could address these risks, including lack of awareness of appropriate PETs, commercially deployable protocols or standards, and lack of demonstrated proof of performance and scalability.

The NPO is soliciting applications to fund projects that are intended to overcome the PETs implementation barriers while advancing the NSTIC vision. NIST anticipates that awards will be in the range of approximately $750,000 to $1,500,000 per year per project for up to two years. NIST anticipates funding new pilots with total funding of up to approximately $2.5 million.

Applications must be received through grants.gov by 11:59pm ET Thursday, May 28, 2015. The NSTIC funding opportunities website contains additional information.

ITL Releases Big Data Interoperability Framework for Review and Public Comment

ITL recently released seven volumes of the NIST Big Data Interoperability Framework for review and public comment. The NIST Big Data Public Working Group (NBD-PWG) produced these documents with extensive participation by industry, academia, and government from across the nation. The scope of the NBD-PWG involves forming a community of interests from all sectors, including industry, academia, and government, with the goal of developing consensus on definitions, taxonomies, secure reference architectures, security and privacy, and from these developing a standards roadmap. Such a consensus would create a vendor-neutral, technology- and infrastructure-independent framework that would enable Big Data stakeholders to identify and use the best analytics tools for their processing and visualization requirements on the most suitable computing platform and cluster, while also allowing value-added from Big Data service providers.

The seven volumes, each of which addresses a specific topic, may be found on the NBD-PWG web page. Send comments by **May 21, 2015**, following the instructions provided at the website.

ITL and Stanford University Host Workshop to Improve Cybersecurity and Consumer Privacy

ITL and Stanford University, in coordination with the White House Summit on Cybersecurity and Consumer Protection, recently hosted a workshop with more than 100 chief technology, information, and security executives to discuss the challenges they face in implementing advanced cybersecurity and privacy technologies in consumer-facing organizations. ITL's National Cybersecurity Center of Excellence (NCCoE) played a large part in organizing the workshop and setting the agenda. The workshop helped to prioritize the key challenges U.S. businesses face in developing strong cybersecurity and privacy programs; identify gaps related to the adoption and use of cybersecurity standards, technologies, and best practices; and gain input into prioritization of NIST's cybersecurity activities to maximize relevance and impact.

ITL Presents Workshop on Likelihood Ratios for the Interpretation of DNA Evidence

ITL statistician Simone Gittelson recently gave a workshop on likelihood ratios for the interpretation of DNA evidence to the Arizona Department of Public Safety. The 30 participants came from three different DNA laboratories in Arizona and consisted of both experienced DNA analysts and training analysts. The two-and-a-half-day workshop covered presentations and exercises on the fundamentals of likelihood ratios and how to present likelihood ratios, likelihood ratios for single-source DNA traces, likelihood ratios for mixtures, the semi-continuous model for likelihood ratios, the continuous model for likelihood ratios, the impact of the number of contributors and a correct or incorrect assumption of the number of contributors on the likelihood ratio, and how to formulate the appropriate pair of propositions.

Staff Accomplishments

Donna Dodson, ITL's Chief Cybersecurity Advisor and Director of the National Cybersecurity Center of Excellence, was recognized by *FedScoop* as one of DC's top 50 Women in Technology for 2015. She is recognized for her work with industry, academia, and other government agencies to forge a consensus on how best to secure the nation's information and communications infrastructure.

Ari Schwartz, ITL's Senior Internet Policy Advisor on detail to the Executive Office of the President as the Senior Director for Cybersecurity, National Security Council, received a Federal 100 Award from Federal Computer Week. The award recognized his deep knowledge and voice of reason as an inside advocate for a wide range of cybersecurity activities.

Daniel Benigni, a recent retiree from ITL's Computer Security Division, received a Lifetime Achievement Award from the InterNational Committee for Information Technology Standards (INCITS). INCITS recognized Benigni's numerous contributions to the INCITS/CS1 - Cyber Security standards community. He participated in INCITS standards activities for more than ten years and served as INCITS/CS1 Chairman during the majority of his tenure.

Selected New Publications

[Supply Chain Risk Management Practices for Federal Information Systems and Organizations]

By Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol
NIST Special Publication 800-161
April 2015

This publication provides guidance to federal agencies on identifying, assessing, and mitigating information and communication technologies (ICT) supply chain risks at all levels of their organizations. The publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities.

[Considerations for Identity Management in Public Safety Networks]

By Nelson Hastings and Joshua Franklin
NISTIR 8014
March 2015

This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety use. These considerations are scoped into the context of their applicability to public safety communications networks with a particular focus on the nationwide public safety broadband network (NPSBN) based on the Long Term Evolution (LTE) family of standards. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process. While specific identity management technologies are analyzed, the document does not preclude other identity management technologies from being used in public safety communications networks.

[Public Safety Mobile Application Security Requirements Workshop Summary]

By Michael Ogata, Barbara Guttman, and Nelson Hastings
NISTIR 8018
January 2015

This document captures the input received from the workshop entitled "Public Safety Mobile Application Security Requirements," which was held in February 2014. The workshop was organized by the Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and the Department of Commerce. This first-of-its-kind workshop was attended by public safety practitioners, mobile application developers, industry experts, and government officials who contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications.

[Assessing Effects of Asymmetries, Dynamics, and Failures on a Cloud Simulator]

By Kevin Mills, James Filliben, and Christopher Dabrowski
NIST TN 1857
March 2015

This paper characterizes the effects of asymmetries, dynamics, and failures when introduced into a cloud computing simulator, which had previously been characterized under static, homogeneous configurations with various patterns of demand and supply. Researchers wanted to determine whether injecting these new factors into the cloud simulator causes fundamental shifts in macroscopic behavior and user experience. They found that introducing asymmetries, dynamics, and failures into the cloud simulator does not induce fundamental shifts in the factors driving simulator behavior, but these new parameters do exhibit interactions with the main driving factors, and with each other. Findings suggest that a previous study, using the cloud simulator to compare virtual-machine placement algorithms, need not be extended to consider the effects of asymmetries, dynamics, and failures. These findings also increase confidence in results from the previous study.

[Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium]

By Celia Paulsen
NISTIR 8041
April 2015

Direct Digital Manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention. It includes Additive Manufacturing (AM), 3D printing, and rapid prototyping. The technology is advancing rapidly and has the potential to significantly change traditional manufacturing and supply chain industries, including for information and communication technologies (ICT). On February 3, 2015, ITL hosted a symposium to explore cybersecurity needed for DDM, to include ensuring the protection of intellectual property and the integrity of printers, elements being printed, and design data. Speakers and attendees from industry, academia, and government discussed the state of the industry, cybersecurity risks and solutions, and implications for ICT supply chain risk management.

[NSTIC Pilots: Catalyzing the Identity Ecosystem]

By Katerina Megas, Phil Lam, Ellen Nadeau, and Colin Soutar
NISTIR 8054
April 2015

Pilots are an integral part of the National Strategy for Trusted Identities in Cyberspace (NSTIC), issued by the White House in 2011 to encourage enhanced security, privacy, interoperability, and ease of use for online transactions. This document details summaries and outcomes of NSTIC pilots; in addition, it explores common themes in the pilots' work developing and operating innovative identity solutions.

Upcoming Technical Conferences

Tattoo Recognition Technology – Challenge (Tatt-C)
Date: June 8, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: None

Launched in September 2014, the Tatt-C activity challenges the commercial and academic community in advancing research and development into automated image-based tattoo matching technology with goals to determine which methodologies are most effective and whether any are viable for identified operational use cases. The workshop will bring together Tatt-C participants from industry and academia and key sponsors and stakeholders to discuss current tattoo detection and matching performance and successes/technical challenges; share utility and perspectives on the operational use of tattoos; identify gaps and needs to support and progress future development; and shape the follow-on evaluation activity.

NIST contact: Mei Lee Ngan

Workshop on Elliptical Curve Cryptography Standards
Dates: June 11-12, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $45 (includes coffee breaks/refreshments)
No cost (without catering service)

Elliptic curve cryptography will be critical to the adoption of strong cryptography as we migrate to higher security strengths. The workshop will provide a venue to engage the crypto community, including academia, industry, and government users, to discuss possible approaches to promote the adoption of secure, interoperable and efficient elliptic curve mechanisms.

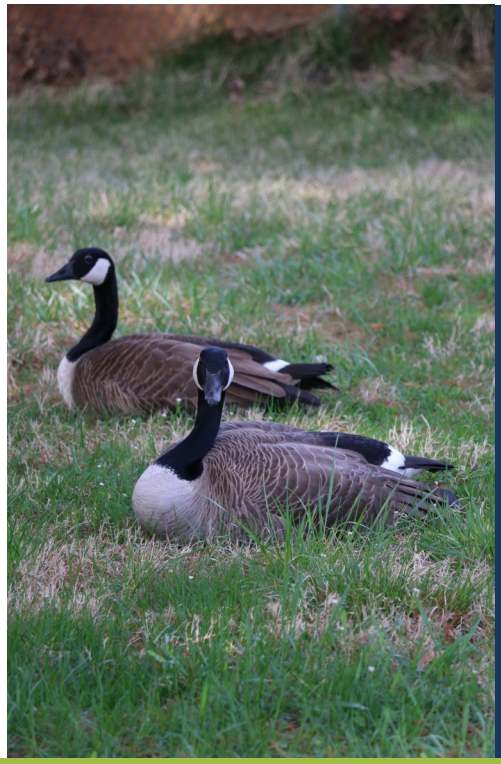
NIST contact: Dustin Moody

Lightweight Cryptography Workshop 2015
Dates: July 20-21, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $55 (includes coffee breaks/refreshments)
$20 (no coffee breaks/refreshments)

When current algorithms can be engineered to fit into the limited resources of constrained environments, their performance is typically not acceptable. NIST seeks to discuss issues related to the security and resource requirements of applications in constrained environments, and potential future standardization of lightweight primitives.

NIST contact: Kerry McKay

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.



Geese nesting time on the NIST Gaithersburg, MD campus
Credit: Katherine Green

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO ITL HOMEPAGE